Communication et organisation

29 | 2006
Figures de l'urgence et communication

Plans de secours d'information et gestion de crise en situation d'urgence : une culture du risque à construire

Brigitte Juanals et Jacques Perriault

Édition électronique
URL : http://journals.openedition.org/communicationorganisation/3379
DOI : 10.4000/communicationorganisation.3379
ISSN : 1775-3546

Éditeur
Presses universitaires de Bordeaux

Édition imprimée
Date de publication : 1 juin 2006
Pagination : 93-106
ISSN : 1168-5549

Référence électronique
Brigitte Juanals et Jacques Perriault, « Plans de secours d'information et gestion de crise en situation d'urgence : une culture du risque à construire », *Communication et organisation* [En ligne], 29 | 2006, mis en ligne le 19 juin 2012, consulté le 30 avril 2019. URL : http://journals.openedition.org/communicationorganisation/3379 ; DOI : 10.4000/communicationorganisation.3379

Plans de secours d'information et gestion de crise en situation d'urgence : une culture du risque à construire

Brigitte Juanals et Jacques Perriault

1 Une enquête du cabinet de consultants *Ernst & Young* sur la sécurité des systèmes d'information dans les entreprises françaises en 2003, menée auprès de 1430 entreprises dans le monde, dont 53 en France, révèle que *« malgré une multiplication importante des risques dont les origines sont aussi bien extérieures qu'internes aux entreprises, seulement 47 % d'entre elles estiment être suffisamment préparées en cas de sinistre majeur »* (Leblond T., 2004). Selon la même étude, *« plus de la moitié des entreprises françaises reconnaissent avoir subi, au cours des douze derniers mois, un arrêt non planifié de leur système d'information ayant provoqué une interruption de service ou de processus critique pendant plus de deux heures »*. T. Leblond (Erst & Young) souligne que *« dans leur recherche permanente pour une rentabilité accrue, les entreprises sont amenées à faire des choix d'organisation les rendant plus vulnérables aux interruptions même mineures »*, comme, par exemple, la spécialisation des sites par fonction (centre de service partagé sur des processus achat, comptabilité, ...), l'externalisation de fonctions, la mise en commun de moyens entre plusieurs entreprises, l'interdépendance plus forte des sites.

2 Dans la même direction, Nicole Aubert et Christophe Roux-Dufort (Aubert N. Et Roux-Dufort C., 2003) dénoncent le « culte de l'urgence » dans les pratiques de management des entreprises. En se conformant aux préconisations des marchés financiers, elles fonctionnent avec des objectifs à court terme et la recherche d'une rentabilité maximale. Une forme de dictature du « temps réel » et de l'urgence s'est infiltrée dans les pratiques quotidiennes. Ainsi, la culture d'entreprise et l'économie de marché ont progressivement imposé au monde une conception occidentale du temps liée à une perception linéaire ; le temps se vit comme une succession d'échéances jusqu'à la mort, par opposition à une conception cyclique rencontrée dans les pays africains et asiatiques. Les outils techniques

ont accompagné cette évolution : les messageries électroniques et les téléphones portables qui maintiennent une pression permanente, les systèmes de production en temps réel, les systèmes d'information fournissant des indicateurs en temps réel, les systèmes de gestion en flux tendus...

3 Les préoccupations récentes des entreprises concernant des plans de continuité d'activité (PCA) en cas de crise ou de catastrophe semblent également dictés par une logique financière. Les aspects de risque et de contrôle interne concernent directement la continuité d'activité, qui est un critère *« de plus en plus pris en compte par les investisseurs et les régulateurs »*, comme en témoignent la Loi de Sécurité financière, le Code du Commerce, les recommandations de l'AMF (Autorité des Marchés Financiers) et le règlement CRBF 2004-02 (Comité de la réglementation bancaire et financière) (Leblond T., 2004)

Un foisonnement des plans de continuation d'activité (PCA)

4 Depuis deux ans, la presse informatique et de *management* accorde une large place aux plans de continuation d'activité (PCA) ou aux plans de reprise d'activité (PRA), qui sont abordés dans leurs différentes dimensions : équipement technique, coûts, processus de mise en oeuvre. Le PCA distingue plusieurs étapes qui rejoignent des démarches de gestion de projet ou de résolution de problèmes : la définition des objectifs, l'analyse des besoins, l'évaluation des risques, le choix de solutions qui déterminent une stratégie de continuité d'activité, l'application de cette stratégie et la réalisation de tests – à faire de manière régulière. Les objectifs sont centrés sur le redémarrage des activités de l'entreprise dans un délai réaliste – mais le plus court possible – et sur la satisfaction des clients. La définition d'une stratégie de continuité s'appuie sur toute une série de plans déclinés par activité ou par objectif : plan de réduction des risques, plan de continuité, plans de contournement, plan de retour à la normale (Leblond T., 2004) ; plan de continuité opérationnelle, plan de continuité informatique (Hamon, 2005). De nouvelles pratiques apparaissent, tel « l'audit de sensibilité au risque », également appelé « audit de vulnérabilité » qui s'applique à toutes les activités de l'entreprise et détermine un « objectif de couverture de risque » (Hamon B., 2004).

5 Les analyses et les solutions informatiques abondent pour guider la démarche technique d'un plan de reprise et des choix possibles, qui dépendent de besoins prioritaires différents en fonction du secteur d'activité : reprendre l'activité au plus vite (pour exemple, un site de vente en ligne) ou éviter de perdre des données (pour exemple, un service de traitement de chèques) (Jacquot T., 2005). Ces priorités sont exprimées en termes de RTO, *Recovery Time Objective* (le délai maximum supporté par l'entreprise avant de reprendre son activité) ou de RPO, *Recovery Point Objective* (la durée maximum d'enregistrement des données qu'il est envisageable de perdre en cas de panne). Les systèmes de réplication, en ligne et à distance (sur une fibre dédiée ou via les réseaux IP) (Berdot, 2004), synchrone ou asynchrone, sont complétés par des sauvegardes classiques de données moins importantes.

Une mobilisation en interne des organisations

6 Sur le plan humain, le PCA fait appel au personnel de l'entreprise ; il suppose l'implication de la direction générale, des directions par métiers, de la direction en charge de la sécurité. Un nouveau profil de poste est apparu, le « responsable de projet PCA », qui est chargé de la gestion du projet de crise dans son ensemble. La constitution de groupes est organisée au moyen de « comités de pilotage », de « cellules de crise » et de « comités projet ». En dehors du personnel, les clients de l'entreprise sont aussi pris en compte puisqu'il s'agit de les « satisfaire » en assurant le plus vite possible la reprise des services attendus. Toutefois, la population présente dans les environs de l'entreprise n'est jamais évoquée dans ces plans alors qu'elle peut être touchée par les conséquences d'une interruption de service. De même, les relations avec l'environnement extérieur sont rarement envisagées ; les commentaires les concernant restent floues et centrées sur les préoccupations de l'organisation : il peut s'agir de « mener des actions préventives de réduction de risques exogènes » (Hamon, 2004), d'établir une « cartographie des échanges » (sur les métiers, les processus, les outils du SI) analysant les « interactions en interne comme en externe » (Leblond, 2004).

Une conception réductrice des sinistres

7 Les types de sinistres envisagés sont variés, allant d'une simple panne ou d'une grève jusqu'à un accident, une dégradation physique ou une destruction de site. Mais peut-on prévoir le même type de PCA quel que soit le risque considéré ? Une inondation, un accident, voire un sinistre majeur, ne nécessitent pas les mêmes solutions, ni les mêmes investissements techniques et humains. Or, selon *XP Conseil*, les entreprises ont tendance à prendre en compte les sinistres partiels et localisés car ils sont identifiés comme étant les plus fréquents ; dans ces situations, *« une architecture de sauvegarde, la redondance de moyens et la technologie de haute disponibilité permettent de garantir la disponibilité d'une application face à de tels sinistres. [...] A contrario, la prise en compte de sinistres régionaux est en général délaissée alors qu'ils représentent 40 % des sinistres déclarés selon une étude de décembre 2001 du Gartner »* (Tête F. et Gronier L., 2004). C'est un véritable plan de secours (d'un coût de 5 % à 10 % du budget informatique) qui devrait être prévu, composé de *« moyens techniques de secours (ordinateurs, équipements de réseau, accès à la messagerie, bureaux équipés, ...), et également d'une structure de gestion de crise, de la planification des différentes actions prêtes à être exécutées, des procédures formalisées et testées »*. Ces mêmes consultants signalent qu'il existe, aux Etats-Unis et en Grande-Bretagne, des sites de secours enterrés pouvant héberger des ressources et des utilisateurs sinistrés.

8 Une fois mis en place, il est essentiel que le plan suive les évolutions de l'entreprise car il est « vivant » de la même manière que les ressources techniques et humaines d'une organisation. Malheureusement, XP Conseil dresse un *« constat alarmant »* concernant les plans de secours qui, *« lorsqu'ils existent, sont en général mal testés, irrégulièrement ou pas du tout. Un plan, non suffisamment testé, reste une coquille vide et un danger puisqu'il fait naître l'illusion de la sécurité »*.

9 Même s'ils répondent à l'origine à des exigences règlementaires et financières, les PCA ou les PRA présentent l'avantage de sensibiliser les organisations à la possibilité d'une exposition à des risques et à leur fragilité face à des événements imprévus. La

détermination des moyens techniques et budgétaires est un paramètre essentiel car il détermine le degré de sécurité qui sera choisi. Même lorsqu'elles s'engagent dans des PCA, ce qui représente encore une pratique minoritaire, les entreprises semblent réticentes à mettre en place un véritable plan de secours car il est coûteux et nécessite une gestion dans le temps ; sa présence dans une entreprise est donc loin de garantir une continuité d'activité en cas de catastrophe. Enfin, la prise en considération de l'environnement extérieur semble très insuffisante et la population vivant à proximité du site n'est jamais évoquée.

Problèmes de communication entre les acteurs et avec la population

10 Les cas de catastrophe qui restent dans la mémoire collective relèvent de situations extrêmes : les attentats de New York (2001), de Madrid (2004) ou de Londres (2005), l'ouragan Katrina à la Nouvelle-Orléans (2004), le séisme du Pakistan... Sans banaliser des situations de cette gravité, nous savons que des perturbations climatiques d'ampleur variable (crues, inondations, tempêtes, canicules...) sont amenées à se développer dans les prochaines années en raison du réchauffement de la planète. Des pannes technologiques sont également susceptibles d'advenir de manière récurrente, les infrastructures électriques ou de télécommunications étant de plus en plus denses et sophistiquées (en 2003, des interruptions d'électricité ont touché plusieurs pays européens – l'Italie, le Royaume-Uni, l'Espagne, le Danemark, la Suède –, les Etats-Unis et le Canada).

Organisations, entreprises et catastrophes

11 En dehors des situations de crise liées à des phénomènes naturels ou à des questions politiques, où elles ont le statut de victime, les entreprises sont susceptibles, elles aussi, d'être à l'origine de catastrophes industrielles. Pour exemple, l'industrie chimique a montré à quel point elle pouvait se révéler dangereuse pour l'environnement et la population : en juillet 1976, le nuage de toxine échappé de l'usine chimique Icmesa (Seveso, Italie) a été la plus grave catastrophe écologique d'origine chimique. Le 3 décembre 1984, à Bhopal (Inde), une fuite de gaz dans une unité de production de pesticides appartenant à Union Carbide a fait 3 800 morts. Le 21 septembre 2001, l'explosion de l'usine AZF de Toulouse a fait 30 morts, 2 500 blessés, et détruits 20 000 logements[1]. Certes, ces accidents présentent un caractère exceptionnel qui caractérise leur rareté. Toutefois, ils montrent également à quel point la population et l'environnement extérieur aux entreprises sont fragilisés par les activités de ces dernières. La mise en place et le suivi de PRA ou de PCA, dans des entreprises pour lesquelles un dérèglement d'activité (sous l'effet d'une interruption, d'une panne, d'un accident...) peut s'avérer problématique pour la sécurité de la collectivité, à petite ou à grande échelle, relève de l'intérêt public.

L'implication de divers réseaux d'acteurs

12 En dehors de la population présente dans une zone sinistrée, il existe beaucoup d'autres acteurs impliqués dans la gestion d'une catastrophe – des entreprises, des unités

spécialisées d'intervention de sécurité ou de santé, des organisations non gouvernementales, des représentants des autorités locales ou nationales, etc. H. Denis distingue les organisations établies orientées vers l'urgence (services médicaux d'urgence – SAMU, SMUR[2] –, sécurité civile – sapeurs pompiers, SDIS[3] –, etc.), les organisations permanentes qui sont des groupes constitués mais non spécifiquement orientés vers l'urgence (représentants de la sécurité civile – maire, préfet... –, police, gendarmerie, militaires...), les organisations en émergence (en particulier les médias) (Denis H., 2002). Ces acteurs éprouvent également, pour des raisons complexes et variées (de nature politique, économique, institutionnelle, sociologique, culturelle...), des difficultés à communiquer entre eux. Ils constituent dans notre problématique une *« communauté temporaire »*, dans laquelle le rôle accordé à la population, notamment d'informateur, a été jusqu'à présent systématiquement négligée.

13 H. Denis évoque à cet égard la nécessité de développer une *« culture de sécurité civile »* consistant à partager les responsabilités de gestion entre les différents niveaux gouvernementaux, les entreprises privées et la population (Denis H., 2002). En dépit des dissensions et des clivages qui peuvent exister entre ces catégories d'individus présents sur le site au moment et après une crise grave, ils constituent malgré tout une *« communauté temporaire »*, appelée à coopérer jusqu'au retour à une situation considérée comme étant à peu près normale. Enfin, dans l'espace public, les médias sont appelés à jouer un rôle clé de relais de l'information (concernant l'évolution de la crise, les décisions prises...) auprès de la population qui demande à être informée en temps réel ; toutefois, cette mission n'est pas toujours facile.

Des moyens de communication inadaptés

14 Dans le cas l'explosion de l'usine AZF de Toulouse (Peton Klein D., rapport ministériel, 2002, p. 32-34), les « informations retransmises par les médias n'ont pas permis durant les premières heures de renseigner de façon objective sur la nature de cet événement ; ces informations ayant même été perçues pour certaines d'entre elles comme contradictoires ». Les moyens techniques qui permettraient de faire face au besoin de disposer d'une information fiable et régulière sur les événements et leur évolution restent à définir (la réquisition d'une chaîne de radio locale ou de tout un autre moyen de communication est à l'étude). De manière générale, cette crise a fait apparaître la nécessité, pour l'ensemble des organisations impliquées dans sa gestion, de mettre en place des moyens de communication en dehors des structures classiques : « L'ensemble des institutions ont fait part de leur constat d'isolement durant cette journée (au moins jusqu'à 17h), cet isolement pouvant se caractérisé par : une absence d'information sur les causes de cet événement, source d'inquiétude et d'angoisse ; l'absence d'information pour certaines d'entre elles quant à la conduite à tenir, face à la nécessité de prendre rapidement des décisions d'organisation pour répondre aux urgences, sans connaissance précise du schéma général d'organisation des secours ». Ce constat est aussi lié à l'organisation générale des services de l'état appelés à collaborer dans l'urgence ; la demande récurrente de tous les acteurs concernant une « organisation des circuits d'information ascendants, descendants et transversaux » pose la question du « partage des compétences et des responsabilités des services de l'état ». La préparation des acteurs à la gestion de la crise a semblé insuffisante. Ce constat, combiné au cloisonnement des

administrations centrales, apparaît également dans le rapport d'information concernant la canicule de l'été 2003 en France (Flandre H., Lepeltier S., Létard V., 2004).

Des paramètres discriminants : les strates d'un milieu désorganisé et les degrés d'une crise

15 Les plans de secours d'information des différents acteurs évoqués ci-dessus font apparaître, au sein de la complexité de situations qu'il conviendrait d'approfondir, des problèmes récurrents. Au-delà des définitions, la description et la conceptualisation du milieu dans lequel survient un événement perturbateur et des degrés que peut comporter une crise semblent essentiels pour amorcer une réflexion sur des plans de secours d'information, dans l'objectif d'identifier des paramètres discriminants à prendre en compte. Ces éléments ont été présentés dans un article précédent (Juanals B., Perriault J., 2005), dont nous allons reprendre, en les complétant, les points essentiels.

La notion de « milieu désorganisé »

16 En partant du constat que tout milieu d'activité humaine est potentiellement désorganisable, nous avons transposé dans cet espace de problème la notion générique de « *milieu désorganisé* »[4] pour décrire un environnement dans ses caractéristiques physiques, matérielles, humaines et culturelles. Dans cette acception, un milieu désorganisé comporte des éléments physiques naturels (sols), des artefacts (infrastructures, bâtiments, etc.) et des êtres vivants (personnes, animaux, germes) ; en ce qui concernent les humains, leurs organisations et leurs composantes idéelles sont particulièrement prises en compte. Sur un plan formel, ce milieu est composé de trois strates. La première strate correspond à la structure géologique, à l'infrastructure du sol et du sous-sol où peuvent arriver des accidents multiples, naturels – séismes, inondation, pollution de la nappe phréatique... – ou artificiels – destructions souterraines, ruptures de canalisations, etc. La deuxième strate, de surface, comprend, d'une part, les équipements (infrastructures, immeubles, etc.), et, d'autre part, les populations ; les perturbations peuvent provenir de l'environnement (pollution), des équipements (destructions liées à un séisme ou à un attentat, explosions accidentelles..) ou de la population (épidémies). La troisième strate est composée de problèmes à résoudre, par des procédures appropriées, pour corriger ou atténuer les déséquilibres mis en évidence ; les composantes informationnelles et communicationnelles y sont très importantes. Ces problèmes sont fondés sur des constats, des représentations constituées à partir d'éléments objectifs et subjectifs, de supputations, d'hypothèses, d'inférences diverses ; il peut s'agir de localiser les membres des groupes dispersés ou des personnes ensevelies, soigner les blessés, trouver des trajets parmi des décombres, de rétablir des télécommunications, de restaurer un minimum de cohésion sociale... Dans cette modélisation, des perturbations peuvent survenir dans chacune des trois strates et avoir des répercussions les unes sur les autres ; de même, des éléments appartenant à des strates différentes peuvent se trouver en interaction, ce qui montre la complexité d'un tel environnement.

Des niveaux de perturbation variables

17 Dans cet environnement, le niveau de perturbation constitue également un paramètre essentiel mais il semble encore, à l'heure actuelle, insuffisamment pris en compte ou minimisé. En complément des nombreuses contributions cherchant à définir la notion de crise (Guilhou X., Lagadec P., 2002), la problématique de la crise est envisagée ici en rapport avec les SI et la gestion de l'information. Dans ce domaine, il existe trois grandes catégories de crises : la situation de crise limitée au domaine de la gestion de l'information et des documents (pertes de données, dégradation de supports, accident limité, etc.) ; la situation de crise dans un autre domaine mais qui touche aussi la gestion de l'information (fermeture de site, attaque virale du SI...) ; les situations de crise plus larges (incendie de site, inondation...) (Buscal C., 2005). Le cas de crise le plus grave est rarement envisagé, en particulier une situation de catastrophe, consistant en un renversement destructif et brutal de l'ordre pré-établi d'un ensemble matériel et humain, avec disproportion entre les besoins et les moyens. Par ailleurs, il faut envisager la possibilité de cumuls de catastrophes, subséquentes ou d'origines distinctes, advenant de manière séquentielle, parallèle ou imbriquée : des événements récents (Turquie, 2002 ; Madrid, 2004) ont montré qu'une crise n'en excluait pas une autre, susceptible d'advenir sur un même lieu ou sur un site distant. Pour exemple, le tsunami, par son onde de choc, a créé de manière simultanée un grand nombre de milieux désorganisés, dans lesquels les trois strates contenaient des éléments parfois très contrastés : dans certaines îles, les problèmes dominants étaient de soigner les blesser tandis que dans d'autres, en Indonésie notamment, il s'agissait de trouver les cadavres, de les identifier et de leur donner une sépulture.

Vers la conception de systèmes d'information en milieu désorganisé acentrés, en lien avec tous les acteurs

18 Les SI classiques ne sont le plus souvent pas adaptés à la gestion de crises graves. Ce sont des dispositifs d'information complexes qui ont été pensés dans un environnement naturel stable, en fonction des modalités habituelles – techniques et sociales – de communication dans la société. Un milieu désorganisé, généré par une situation de catastrophe, rend impossible leur utilisation, du fait même de la détérioration ou de la destruction des infrastructures techniques sur lesquelles ils reposent ; Ces considérations nous ont amenés à élaborer la notion de « *système d'information en milieu désorganisé* » (SIMD). Un SIMD est une organisation de recueil, de stockage, de traitement et de redistribution de l'information qui aide une collectivité ayant subi une catastrophe à se construire progressivement une représentation globale et une prise de conscience concomitante de ce qui s'est passé, de ce qui est en train de se passer, des conséquences déjà constituées et des évolutions en cours dans les trois strates identifiées (Juanals, Perriault, 2005). L'échange d'informations s'effectue dans une situation anormale d'urgence, de stress et d'incertitude.

Une connectivité technologique de substitution

19 Un SIMD aide à constituer et à gérer une communauté de savoir sur une catastrophe grâce à la mise en place d'une connectivité technologique. Principalement alimenté (et utilisé) par la population présente sur le site, qui est considérée comme une composante majeure du dispositif, il permet de rechercher et de diffuser des savoirs à partager et, si nécessaire, de les construire. Son concours immédiat et actif est nécessaire pour enrichir la connaissance collective de la situation (les perturbation survenues ou en train d'avoir lieu) et la partager à l'intérieur et à l'extérieur – notamment en direction des autorités et des médias – du site, pour autant qu'un système d'information ait pu être rapidement mis en place. La population est considérée comme un producteur d'informations dans les trois strates du milieu désorganisé ; elle n'est plus seulement demandeuse d'informations, ce qui donne un rôle positif aux victimes et permet de raccourcir sensiblement la fourniture et l'exploitation d'informations locales. Tout acteur sur le site devient une composante – active ou passive – du système d'information.

20 Lors des séismes de Gumri (Arménie, 1988) et de Boumerdès, les enquêtes conduites par le laboratoire CRIS-SERIES auprès de victimes ont fait ressortir que la totalité des équipements de télécommunications (strate 2) étaient hors d'usage, alors qu'un besoin énorme de communications de proximité se faisait sentir. En pareil cas, à peu près partout dans le monde, le protocole mis en place est similaire : après un temps assez long (de deux à quatre jours en cas de séismes), des unités d'intervention spécialisée arrivent sur le terrain et installent des dispositifs provisoires de télécommunication pour communiquer entre elles. En France, les unités spécialisées d'intervention (Sapeurs pompiers, Armée, Protection Civile, SAMU, Gendarmerie Nationale) disposent de leurs propres dispositifs d'information et de communication. Sur le site de Boumerdès, la société française TD Com a fourni des portables GSM à la population tout en établissant des cellules provisoires de télécommunication : l'innovation a résidé dans la fourniture de moyens de communication à la population, cette dernière étant habituellement exclue, à notre connaissance, de l'ensemble des systèmes de communication en urgence sur un site désorganisé.

Dispositif de plateforme et dispositif acentré

21 Dans le but d'intégrer tous les acteurs – en particulier la population – qui constituent la *« communauté temporaire »*, créée lors d'une crise, en tant que composants d'un dispositif d'information et de communication, le laboratoire CRIS-SERIES envisage l'élaboration de deux scénarios : l'un comporte un SI appuyé sur une plateforme, l'autre est de type « net-centric » ou net-centré – terminologie préférée ici à celle de SI a-centré (les spécifications techniques ne sont pas indiquées dans cet article). Dans les deux cas, la médiation humaine des échanges sur le site joue un rôle central, la communication orale est prioritaire, et la population est dotée de téléphones GSM utilisant une fréquence et des cellules provisoires. Ces dispositifs entrent dans la catégorie des *« mobile ad hoc network systems »* (MANETS)[5], qui sont des réseaux de plateformes mobiles, indépendants des infrastructures de communication préexistantes ou fixes, pouvant assurer des fonctions de transmission et de relais d'informations. De plus, pour faire face à des superpositions possibles de catastrophes, le système d'information doit intégrer, sur le plan logistique,

une nécessité d'ouverture et d'extension, qui peut être réalisée par l'ajout de ramifications au système existant ou par sa connexion avec un second dispositif, mis en place pour faire face aux événements les plus récents. Une connectivité aisée, reposant sur des standards identiques, est nécessaire.

22 Dans le système d'information porté par une plateforme, la médiation humaine et la communication orale s'effectuent depuis et vers un centre de télé accueil embarqué, qui est le cœur du dispositif de télécommunication installé sur le site après la catastrophe. Le télé accueil et les constituants du dispositif en réseau (des téléphones cellulaires à la disposition de la population, des bornes interactives disséminés sur le site, des micro caméras, des générateurs d'électricité) sont mobiles et sont déplacés en fonction des circonstances. Dans la version net-centrée, le système d'information est un cadre de travail pour toute la connectivité et l'interopérabilité technique et humaine. Il permet à tous les utilisateurs et aux partenaires de missions de partager les informations dont ils ont besoin, quand ils en ont besoin, sous une forme qui leur est compréhensible, ce qui leur permet d'agir avec confiance et protège l'information de ceux qui ne doivent pas y accéder. Le cœur du système net-centré est un téléphone portable (ou tout autre outil de communication nomade) doté d'un canal dédié aux situations de catastrophe. Il intègre des fonctions de communication et de transmission d'informations en y ajoutant l'accès à l'Internet *via* un moteur de recherche, ce qui permet d'accéder aux bases de données et aux sites utiles en cas d'urgence et de situations imprévues.

23 Après une crise grave, le quadrillage géographique de base qui sert de repère au SI n'existe plus, en raison de la privation d'énergie et de la destruction du matériel ainsi que des infrastructures. Construits sur le recours à des appareils et à des réseaux de télécommunication mobiles et indépendants du site endommagé (MANETS), les SIMD rendent possible la constitution rapide d'un SI humain nomade. Appuyé sur des technologies de substitution, un SIMD a pour finalité la continuité ou la reprise de la communication et de l'échange d'informations ; pour les personnes présentes sur le site, il s'agit de rechercher des informations et de communiquer à l'intérieur et en dehors de la zone endommagée (les appels de lampe électrique pendant la nuit sont un exemple de tentative pour communiquer avec l'extérieur). Dans la modélisation d'un tel SI temporaire de crise, l'élément essentiel est humain et se trouve placé au cœur du dispositif ; la technologie est palliative.

Vers une nouvelle conception des SI et des plans de secours d'information

24 Il faut modifier la conception des SI « normaux », qui suppose un environnement et des conditions stables de fonctionnement, de façon à y inclure, non seulement un risque de panne ou de perturbation mineure – ce qui est le plus souvent le cas –, mais un scénario de destruction quasi-totale. Les impératifs de rentabilité, la logique des marchés financiers, l'installation d'une culture de l'urgence et le développement insuffisant d'une culture du risque, peuvent avoir des conséquences néfastes sur les capacités des entreprises et des organisations à prévoir et à faire face à des situations de crise, voire de catastrophe. Un véritable plan de secours d'information, s'il tient compte de perturbations et de destructions exogènes au système d'information – à son architecture, à son fonctionnement matériel, logiciel et énergétique – conduit à renverser la

proposition selon laquelle un SIMD constitue une situation d'exception. La puissance d'un réseau de transport, de communication ou de télécommunication est déterminée sur la base de sa capacité à fonctionner en période de pointe, non en période basse ou normale. Cela conduit à poser la question suivante : dans leur façon de concevoir des crises, n'est-il pas indispensable que les SI adoptent le même principe de fonctionnement, c'est-à-dire qu'ils soient conçus et formatés pour être à même de gérer une situation de catastrophe afin d'assurer d'assurer une continuité, voire une reprise rapide, d'activité ? Ne faut-il pas en corollaire définir la « communauté temporaire », avec tous ses acteurs – y compris les victimes –, en tant qu'utilisatrice de tels systèmes d'information ?

BIBLIOGRAPHIE

Aubert, N., et Roux-Dufort, C. *Le culte de l'urgence*, Paris, Flammarion, 2003.

Berdot V., « Le stockage à distance enfin populaire. Les liaisons dédiées sont trop onéreuses. Le stockage à distance utilise les réseaux IP, une solution bien moins chère. », 01 Informatique, 19/11/2004.

Buscal C., « Plans de secours pour l'information, faire un PRA en avant », Archimag, n° 183, avril 2005.

Denis, H., *La réponse aux catastrophes : quand l'impossible survient*, Montréal, Presses internationales Polytechnique, 2002,

Flandre H., Lepeltier S., Létard V., Rapport d'information n° 195 (2003-2004), fait au nom de la mission commune d'information, *La France et les Français face à la canicule : les leçons d'une crise*, Sénat, déposé le 3 février 2004, en ligne (consultation 26/11/05) : http://www.senat.fr/rap/r03-195/r03-195.html

Guilhou, X., Lagadec, P., « Les conditions de survenue des crises graves » pp. 157-210, in Amalberti R., Fuchs C., Gilbert C. (dir.), *Conditions et mécanismes de production des défaillances, accidents et crises*, CNRS-Maison des Sciences de l'Homme-Alpes, juin 2002.

Hamon B., « Plan de continuité d'activité : quelle démarche adopter ? », zdnet.fr, 09/12/2004, en ligne (consultation 14/11/05) : http://www.zdnet.fr/entreprise/service-informatique/securite/0,50007195,39191691-1,00.htm

Jacquot T., « Reprise d'activité : n'oubliez pas le back-up. L'analyse d'impact doit guider la démarche technique d'un plan de reprise. La sauvegarde peut suppléer la réplication. », 01 Informatique, 05/08/2005.

Juanals B., Perriault J, « Mobilisation immédiate de savoirs en ligne pour des situations d'urgence », Colloque international du 22-24/09/005, Université de Bordeaux 3, laboratoire GRESIC, *Enjeux et usages des TIC. Aspects sociaux et culturels* (dir. Vieira L. et Pinède-Wojciechowski N.), Presses Universitaires de Bordeaux, 2005, tome 1, pp. 21-37.

Leblond T., « Continuité d'activité : les nouveaux enjeux réglementaires et financiers », Ernst & Young, 21/06/2004, en ligne (consultation 14/11/05) : http://www.ey.com/global/content.nsf/France/issues_perspectives_SI_continuite_activite

Peton Klein D., Explosion de l'usine AZF de Toulouse le 21/09/2002, rapport de mission, Paris, La documentation française, 2002.

Tête F. et Gronier L. (XP Conseil), « Avez-vous un PRA ?La recrudescence des perturbations climatiques et énergétiques peuvent mettre en péril l'économie ou avez-vous un plan de reprise d'activité en état de fonctionnement ? », Mags.Securs (Magazine européen de la sécurité informatique), juin 2004, en ligne (consultation 14/11/05) : http://www.mag-securs.com/article.php3?id_article=972

NOTES

1. Mamou Yves, « Une série de catastrophes ont sensibilisé l'opinion », Le Monde, 16/11/2005.
2. Service Mobile de secours et de soins d'urgence.
3. Service départemental d'incendie et de secours.
4. Cette notion est issue de la psychopathologie et de la sociologie, où elle désigne un milieu social dans lequel les modes d'organisation familiale, relationnels notamment, sont fortement détériorés. Cf. Hassan Soubhi, Parminder Raina, Dafna Kohen, Influence du quartier, de la famille et du comportement des enfants sur le risque de blessure au Canada, Direction générale de la recherche appliquée Politique stratégique Développement des ressources humaines, mars 2001.
5. MANET = Mobile ad hoc networks. Voir : Goutham Karumanchi Srinivasan Muralidharan and Ravi Prakash ""Information Dissemination in Partitionable Mobile Ad Hoc Networks, To appear in Proceedings of IEEE Symposium on Reliable Distributed Systems, Lausanne, Switzerland, 20-22, Oct, http://www.ee.surrey.ac.uk/Personal/G.Aggelou/PAPERS/camera.ready.pdf; consulté le 31.05.05

RÉSUMÉS

Placés dans le contexte d'une gestion de crise (politique, économique...) ou de catastrophe (naturelle, sanitaire...), les plans de secours des entreprises en matière d'information et la communication en situation d'urgence se sont développés récemment. Ils posent problème dans la mesure où ils semblent très centrés sur des préoccupations internes et des questions de coût. Ils n'envisagent que rarement un cas de destruction totale sur un site et sont peu préoccupés des liens avec l'extérieur, alors même qu'ils se situent dans l'espace public, ce qui impliquerait la prise encompte des différents acteurs présents sur un site – les autorités civiles, le personnel de secours, les entreprises et la population civile, dont les membres sont à la fois usagers du SI, citoyens et victimes.Une approche différente, construite sur la corrélation entre les systèmes d'information en milieu désorganisé (SIMD) et les plans de secours, serait pourtant plus adaptée. Elle repose sur la modélisation d'un SIMD et sur la communication avec les différents acteurs, y compris la population.

INDEX

Mots-clés : urgence, plan de secours d'information, plan de continuité d'activité (PCA), système d'information, milieu désorganisé, crise, catastrophe

AUTEURS

BRIGITTE JUANALS

Brigitte Juanals est Maître de conférences en Sciences de l'Information et de la communication, Université de Lille 3, laboratoire GERIICO (EA 1060). Mail : brigitte.juanals@club-internet.fr

JACQUES PERRIAULT

Jacques Perriault est Professeur en Sciences de l'information et de la communication à l'Université Paris 10-Nanterre, directeur du laboratoire CRIS-SERIES (équipe d'accueil n ° 1738). Mail : jperriault@free.fr